

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TENNESSEE  
WESTERN DIVISION

---

CONNIE BOANE,	)	
	)	
Plaintiff,	)	
	)	
v.	)	No. 11-2565 AJT/TMP
	)	
JAMES A. BOANE and DONNA	)	
BOANE,	)	
	)	
Defendants.	)	

---

REPORT AND RECOMMENDATION

---

Before the court by order of reference is defendants James A. Boane and Donna Boane's Motion to Dismiss for Failure to State a Cause of Action ("Second Motion to Dismiss"), filed on January 6, 2012. (ECF No. 33.) Plaintiff Connie Boane filed a response in opposition on February 1, 2012. The court recommends that the motion be granted.

**I. PROPOSED FINDINGS OF FACT**

James Boane and Connie Boane were married and are now divorced. James Boane is currently married to Donna Boane. This case arises out of alleged unauthorized access of plaintiff's private health and medical records by the defendants. According to plaintiff, on or about December 21, 2010, she received an e-mail from her health insurance provider, United Healthcare ("United"), informing her that the password to her online account had been

changed. Plaintiff had not requested a change to her password. She subsequently contacted United to have the company investigate why the password had been changed and what records had been accessed. On January 3, 2011, United provided plaintiff with a report summarizing its investigation. This report indicated that, on the date the password was changed, someone had accessed plaintiff's account and viewed approximately fifty online documents, including explanations of benefits, appeal claim notes, account balances, and personal healthcare records. Shortly after viewing these documents, the unauthorized user changed plaintiff's password. The report also included the Internet Protocol ("IP") address of the user who had accessed the account.

At the time of the alleged unauthorized access to plaintiff's account, she and James Boane were involved in post-divorce litigation in Shelby County Chancery Court. On or about January 25, 2011, as part of the divorce litigation, plaintiff had a subpoena issued to BrightHouse Networks c/o Neustar ("Neustar"), seeking production of records that would identify the owner of the computer with the IP address provided in United's report. (See Compl., Ex. B.) On April 15, 2011, the Chancery Court ordered (over James Boane's objection) that Neustar comply with the January 25 subpoena and produce the requested records. (Id.) In response, on April 19, 2011, Neustar produced a business record allegedly showing that the IP address was associated with an account held by

Donna Boane. This business record also showed that the address for the account matched the address of defendants' current residence in Oviedo, Florida.

In her complaint, plaintiff asserts that defendants' alleged unauthorized access of her United account violates the following federal and state statutes: the Stored Communications Act, the Electronic Communication Privacy Act, the Computer Fraud and Abuse Act, the Health Information Portability and Accountability Act, Tennessee Code § 39-13-601, and the Tennessee Personal and Commercial Computer Act of 2003. Plaintiff has also asserted common law claims of intentional infliction of emotional distress, reckless infliction of emotional distress, negligent infliction of emotional distress, invasion of privacy, and negligence.

On August 2, 2011, defendants filed a motion to dismiss ("First Motion to Dismiss"), on the bases of lack of personal jurisdiction, improper venue, and failure to state a claim for which relief may be granted. In the alternative, defendants asked the court to transfer the action to the Middle District of Florida. On December 5, 2011, the district judge denied the First Motion to Dismiss on all grounds.<sup>1</sup> Defendants, however, filed a Motion for

---

<sup>1</sup>This case was originally assigned to former District Judge Bernice B. Donald. Upon Judge Donald's appointment to the Sixth Circuit Court of Appeals, the case was reassigned to Chief Judge Jon P. McCalla on December 29, 2011, and subsequently reassigned again to Judge Arthur J. Tarnow on February 22, 2012. Judge Tarnow referred the current motion to the undersigned magistrate judge on June 5, 2012.

Reconsideration on December 15, 2011. The district judge granted this motion with respect to defendants' arguments pursuant to Rule 12(b)(6) that plaintiff had failed to state a valid claim, and allowed defendants to file a renewed motion on this ground within ten days. Defendants complied with this order and filed the Second Motion to Dismiss currently before the court. In this motion, defendants raise various arguments - substantially the same arguments as those stated in the First Motion to Dismiss - against each of plaintiff's federal statutory claims and her claim for violation of Tennessee Code Annotated § 39-13-601. Defendants have not, either in their current motion or the First Motion or Dismiss, raised any arguments against plaintiff's remaining state statutory claim (violation of the Tennessee Personal and Commercial Computer Act of 2003) or her common law claims.

## **II. PROPOSED CONCLUSIONS OF LAW**

### **A. Rule 12(b)(6) Standard**

Federal Rule of Civil Procedure 12(b)(6) authorizes the court to dismiss a complaint for failure to state a claim upon which relief may be granted. Fed. R. Civ. P. 12(b)(6). Rule 12(b)(6) tests the sufficiency of the claim for relief, "and as such, it must be understood in conjunction with Rule 8(a), which sets out the federal standard for pleading." Hutchison v. Metro. Gov't of Nashville and Davidson Cnty., 685 F. Supp. 2d 747, 748-49 (M.D. Tenn. 2010) (citing 5B CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL

PRACTICE AND PROCEDURE § 1356 (3d ed. 2004)). In reviewing the complaint, the court construes the complaint in the light most favorable to the plaintiff and must accept all well-pleaded factual allegations as true. La. Sch. Emps.' Ret. Sys. v. Ernst & Young, LLP, 622 F.3d 471, 477-78 (6th Cir. 2010). "Under Federal Rule of Civil Procedure 8(a)'s pleading standard, a plaintiff must provide 'a short and plain statement of the claim showing that [he] is entitled to relief.'" Ashland, Inc. v. Oppenheimer & Co., Inc., No. 10-5305, 2011 WL 3181277, at \*3 (6th Cir. July 28, 2011). "Yet the complaint must include more than 'labels and conclusions' or a 'formulaic recitation of the elements of a cause of action,' . . . and instead proffer 'enough facts to state a claim to relief that is plausible on its face[.]'" Id. (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009).

#### **B. The Stored Communications Act**

Defendants argue that their alleged access of plaintiff's United online account does not constitute a violation of the Stored Communications Act ("SCA") for two reasons. First, they argue that United is not an "electronic communication service" for purposes of the SCA. Second, they contend that the information purportedly

accessed does not fit the statutory definition of "electronic communication."

It is a violation of the SCA to "(1) intentionally access[] without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed[] an authorization to access that facility; and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system[.]" 18 U.S.C. § 2701(a). The SCA provides a private cause of action to any person aggrieved by an intentional violation of the statute:

Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or *other person aggrieved by any violation of this chapter* in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

18 U.S.C. § 2707(a) (emphasis added). The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications[.]" 18 U.S.C. § 2510(15). The Sixth Circuit has never addressed the meaning of this term within the SCA. However, several district courts have done so, and have uniformly found that businesses do not qualify as electronic communication services simply because they utilize the internet or a website that allows customers to access or purchase their products. The court finds particularly persuasive the court's analysis in In re Jetblue

Airways Corp. Privacy Litig., 379 F. Supp. 2d 299 (E.D.N.Y. 2005):

Although JetBlue operates a website that receives and transmits data to and from its customers, it is undisputed that it is not the provider of the electronic communication service that allows such data to be transmitted over the Internet. Rather, JetBlue is more appropriately characterized as a provider of air travel services and a consumer of electronic communication services. The website that it operates, like a telephone, enables the company to communicate with its customers in the regular course of business. Mere operation of the website, however, does not transform JetBlue into a provider of internet access, just as the use of a telephone to accept telephone reservations does not transform the company into a provider of telephone service. Thus, a company such as JetBlue does not become an "electronic communication service" provider simply because it maintains a website that allows for the transmission of electronic communications between itself and its customers.

Id. at 307; see also Copeland v. Northwest Airlines Corp., No. 04-2156, 2005 WL 2365255, at \*2 (W.D. Tenn. Feb. 28, 2005) ("Numerous Courts have found that the term 'electronic communication service' refers to entities that provide internet access to customers, such as internet service providers ('ISP's'), as opposed to merchants and businesses that sell their products or services over the internet."); Dyer v. Northwest Airlines Corps., 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) ("[B]usinesses offering their traditional products and services online through a website are not providing an 'electronic communication service.'").

Plaintiff effectively concedes that United does not qualify as an electronic service provider in her response brief. She argues that "[t]he relevant inquiry, however is whether Defendants

improperly accessed any electronic communication service facility when Defendants accessed without authorization Plaintiff's online health benefits account via the Internet - not whether United Healthcare is an electronic communication service[.]" (See ECF No. 34-1, p. 6) (emphasis in original). Plaintiff goes on to argue that because defendants utilized Road Runner internet service to access her health records without her authorization, they violated the SCA. The court disagrees. Adopting plaintiff's argument would mean that a party would violate the SCA whenever her or she used the internet to access information without authorization.

The court finds instead that this case is similar to those faced by the district courts cited above. United is certainly not an internet service provider, nor does it provide electronic communication services. The court finds, therefore, that United's website does not qualify as "a facility through which an electronic communication service is provided." The court recommends that plaintiff's SCA claim be dismissed. Consequently, it is not necessary to address defendants' second argument under the SCA, that the information accessed within plaintiff's account does not constitute "electronic communication."

**C. The Electronic Communications Privacy Act and Tennessee Code Annotated § 39-13-601**

An individual violates the Electronic Communications Privacy Act ("ECPA") when he or she "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to

intercept, any wire, oral, or electronic communication[.]” 18 U.S.C. § 2511(1)(a).<sup>2</sup> The statute defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). The Sixth Circuit has not addressed the precise meaning of “intercept” within the ECPA. Several circuit courts, however, have done so and found that in order for a violation of the statute to occur, the defendant must have acquired the relevant communication during its transmission or “flight,” as opposed to during its storage. Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) (agreeing with Fifth Circuit that “there can be no ‘intercept’ of an e-mail in storage, as an e-mail in storage is by definition not an ‘electronic communication’”); United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003) (finding no violation of the ECPA because “there is nothing to suggest that any of the information . . . was obtained through contemporaneous acquisition of electronic communications while in flight”); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) (“We therefore hold that for a website such as Konop’s to be ‘intercepted’ in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage.”); Steve

---

<sup>2</sup>The ECPA modified the pre-existing Federal Wire Act (“FWA”), and courts refer to the two acts interchangeably when analyzing claims pursuant 18 U.S.C. § 2511.

Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994) ("Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'"). The court agrees with these decisions.

In this case, plaintiff has not alleged that defendants intercepted any of her electronic communications while they were in transmission. Instead, she alleges only that defendants accessed and viewed her health records while they were stored by United. Plaintiff attempts to address this deficiency in her complaint by arguing:

when the Defendants took steps to create and/or reset Plaintiff's password, it is believed that the new password was sent to both the actual email address of Plaintiff and an email address entered by the Defendants. Rather than being received only by Plaintiff, the electronically transmitted information was contemporaneously received by Defendants and, thereby, communications directed to Plaintiff were contemporaneously intercepted by Defendants.

(Pl.'s Resp. to Second Mot. to Dismiss, ECF No. 34-1, p. 11.) The court finds this to be an overly strained interpretation of contemporaneous interception. In the court's view, simply having an e-mail sent to one address, while an identical second e-mail is sent to another address, does not amount to an "interception" of the first e-mail. The court recommends that plaintiff's ECPA claim be dismissed.

In addition, the Tennessee Wire Act ("TWA"), codified at T.C.A. § 39-13-601 et seq., mirrors the language of the ECPA, and

courts have interpreted the two statutes similarly. Hayes v. Spectorsoft Corp., No. 1:08-cv-187, 2009 WL 3713284, at \*9 (E.D. Tenn. Nov. 3, 2009) ("[C]ourts interpreting both the ECPA and the TWA have interpreted them in the same way using federal case authority due to the dearth of Tennessee cases interpreting the TWA."); Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 979 (M.D. Tenn. 2008) ("This court agrees that whether both the TWA and the FWA have been violated here can be determined based on the FWA and its case law."). The court recommends, therefore, that plaintiff's TWA claim be dismissed.

#### **D. The Computer Fraud and Abuse Act**

Plaintiff has further alleged that defendants have violated the Computer Fraud and Abuse Act ("CFAA"). It is a violation of the CFAA to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). The CFAA further permits any person who suffers damage or loss due to a violation of the statute to bring a civil action against the violator, so long as the alleged conduct involves one of the five factors listed under section 1030(c)(4)(A)(i). 18 U.S.C. § 1030(g). These five factors are:

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security[.]

18 U.S.C. § 1030(c)(4)(A)(i) (hereinafter referred to as the "Additional Factors").

Defendants have raised four arguments against plaintiff's CFAA claim. They argue first that plaintiff does not have standing to assert a CFAA claim for unauthorized access to United's computer system; second, that United's computer system is not a "protected computer" under the statute; third, that defendants did not engage in any unauthorized access; and fourth, that plaintiff has not pleaded any damages recognized under the CFAA. The court will address each of these arguments in turn below.

The CFAA provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief," so long as one of the Additional Factors is present. 18 U.S.C. § 1030(g). Consequently, defendants' argument that plaintiff lacks standing is without merit. Defendants argue that plaintiff cannot pursue a CFAA claim because she "has no property rights or interest in the personal

property of United Health Care." Defendants have not cited, and the court in conducting its own research has not found, any statutory or case authority to support this argument.

In regard to defendants' second argument, a "protected computer" is statutorily defined as a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]" 18 U.S.C. § 1030(e)(2)(B).<sup>3</sup> Other courts have interpreted this definition as including any computer that is connected to the internet. Jole v. Apple, No. 3-11-0882, 2011 WL 6101553, at \*3 (M.D. Tenn. Dec. 8, 2011) ("The Court agrees with those cases which have found that a connection to the internet is affecting interstate commerce or communication."); Cont'l Grp., Inc. v. KW Prop. Mgmt., LLC, 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009) ("A connection to the internet is 'affecting interstate commerce or communication.'"); Paradiqm Alliance, Inc. v. Celeritas Techs., LLC, 248 F.R.D. 598, 602 (D. Kan. 2008) ("[A] computer providing a 'web-based' application accessible through the

---

<sup>3</sup>Although not relevant under the facts of this case, the statute's definition of "protected computer" also includes a computer "exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government[.]" 18 U.S.C. § 1030(e)(2)(B).

internet would satisfy the 'interstate communication' requirement."). This court agrees with these cases and finds that a computer or computer system accessible via the internet qualifies as a "protected computer" under the CFAA. The court therefore rejects defendants' second argument that United's computer system does not qualify as a "protected computer" under the CFAA.

Third, defendants argue that, even assuming that plaintiff's allegations are true, they did not engage in unauthorized access because they accessed United's system "with the authorization of the owner of the computer system." (Memo. in Supp. of Second Mot. to Dismiss, ECF No. 33-1, p. 12.) As stated earlier, the CFAA makes it unlawful to "intentionally access[] a computer without authorization or exceed[] authorized access." While the statute does not define "authorization," the phrase "exceeds authorized access" is defined as, "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The court finds that the complaint sufficiently alleges that defendants have, at the very least, exceeded their authorized access by gaining access to United's website under presumably false pretenses and accessing plaintiff's private health records. For this reason, the court rejects defendants' third argument against plaintiff's CFAA claim.

Finally, defendants argue that plaintiff's CFAA claim must be

dismissed because she has not pleaded any damages recognized under the CFAA. As stated earlier, an individual aggrieved by a CFAA violation, in order to bring a private cause of action, must satisfy one of the five additional factors. Under the first of these factors, the violation must have resulted in "loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). Defendants contend that plaintiff has not pleaded any losses that would satisfy this requirement. In response, plaintiff argues first that she has indeed suffered adequate damages to support her CFAA claim under this factor. In the alternative, plaintiff argues that, even if the first factor is not satisfied, her claim should survive because of the presence of the second factor: "the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals." 18 U.S.C. § 1030(c)(4)(A)(i)(II).

The CFAA defines the term "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). When pursuing a claim based only upon the first of the Additional Factors, the statute adds the additional requirement

that the requisite losses "are limited to economic damages." 18 U.S.C. § 1030(g). The court agrees with defendants that plaintiff has not adequately pleaded the requisite losses to bring a CFAA claim under the first Additional Factor. In her complaint, plaintiff states in regard to damages only that, "[a]s a direct and proximate result of Defendants' knowing, intentional and willful violation of the Computer Fraud and Abuse Act, Plaintiff has sustained damages and is entitled to an award of damages pursuant to 18 U.S.C. § 1030(g)." (Compl. ¶ 37.) Moreover, in the section of her complaint devoted to damages, plaintiff adds only, "[f]or Defendants' violation of the Computer Fraud and Abuse Act, Plaintiff seeks recovery of her economic damages in an amount to be proven at trial." (Id. at ¶ 76.) The court finds that these bare bones allegations do not adequately plead the losses or damages suffered by plaintiff as a result of defendants' alleged CFAA violation. Twombly and Iqbal require that a plaintiff allege enough facts to state a claim to relief that is plausible on its face. Twombly, 550 U.S. at 570. Here, plaintiff has not alleged any facts in the complaint to support a claim for economic damages, such as loss of wages or incurment of medical expenses.

Next, the court must address whether plaintiff's CFAA claim survives under the second Additional Factor regarding modification or impairment of medical treatment. The statute does not define any of the relevant terms within this medical treatment factor. In

addition, this court has been unable to find any case law addressing this factor in any meaningful way. Under a plain reading of the statutory language, the court finds that plaintiff's allegations do not constitute "modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals." While it is true that the records accessed by defendants contained medical information, the complaint does not contain any allegations that defendants' actions resulted in any actual or potential modification or impairment of plaintiff's medical care or treatment. Consequently, the court finds that plaintiff has not alleged sufficient facts to satisfy this factor. As none of the Additional Factors required to support a private civil claim under CFAA are present, the court recommends that plaintiff's CFAA be dismissed.

**E. The Health Information Portability and Accountability Act**

Plaintiff has also brought a claim for violation of the Health Information Portability and Accountability Act ("HIPAA"). Although the Sixth Circuit has not addressed the issue, several other circuit courts and numerous district courts have uniformly found that HIPAA does not provide a private right of action. See Johnson v. Depts. of Army and Air Force, No. 10-16450, 2012 WL 32132, at \*1 (9th Cir. Jan. 6, 2012) ("The district court properly dismissed Johnson's claims under the Health Insurance Portability and

Accountability Act . . . because Johnson did not have a private right of action."); Dodd v. Jones, 623 F.3d 563, 569 (8th Cir. 2010) ("We agree with the district court that this claim fails because HIPAA does not create a private right of action."); Acara v. Banks, 470 F.3d 569, 572 (5th Cir. 2006) ("We hold there is no private cause of action under HIPAA[.]"); Wilson v. Codd, No. 12-91-KKC, 2012 WL 1434966, at \*1 (E.D. Ky. Apr. 25, 2012) ("Private citizens have no standing to sue a covered entity for a violation of HIPAA"); McElyea v. Wallace, No. 3:11-0914, 2011 WL 5444100, at \*4 (M.D. Tenn. Nov. 9, 2011) ("[t]here is no private cause of action under HIPAA[.]") (quoting Acara, 470 F.3d at 571-72); Kogan v. Tenn. Bd. of Dentistry, No. 3:06-00789, 2008 WL 842462, at \*5 n.1 (M.D. Tenn. Mar. 28, 2008) ("[W]hile the Sixth Circuit has yet to address the question, federal courts are in accord that HIPAA is not enforceable through private causes of action.") The court agrees with these decisions, and finds that HIPAA does not create a private cause of action. The court therefore recommends that plaintiff's HIPAA claim be dismissed.

### **III. RECOMMENDATION**

For the foregoing reasons, the court recommends that defendants' Second Motion to Dismiss be granted.<sup>4</sup>

---

<sup>4</sup>As stated earlier, defendants have not argued for dismissal of plaintiff's remaining claims: violation of the Tennessee Personal and Commercial Computer Act of 2003, intentional infliction of emotional distress, reckless infliction of emotional distress, negligent infliction of emotional distress, invasion of privacy, or

Respectfully submitted,

s/ Tu M. Pham  
TU M. PHAM  
United States Magistrate Judge

July 3, 2012  
Date

**NOTICE**

**ANY OBJECTIONS OR EXCEPTIONS TO THIS REPORT MUST BE FILED WITHIN FOURTEEN (14) DAYS AFTER BEING SERVED WITH A COPY OF THE REPORT. 28 U.S.C. § 636(b)(1). FAILURE TO FILE THEM WITHIN FOURTEEN (14) DAYS MAY CONSTITUTE A WAIVER OF OBJECTIONS, EXCEPTIONS, AND ANY FURTHER APPEAL.**

---

negligence. Although defendants move to dismiss the entire complaint, because their motion does not address these remaining claims, plaintiff's complaint should not be dismissed in its entirety.